Ministry of JUSTICE

OFFICIAL

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD QUALIFIED SECURITY ASSESSOR (PCI DSS QSA)

STATEMENT OF REQUIREMENTS

1 Introduction

1.1 Headline Requirements

The Ministry of Justice (MoJ) requires a Qualified Security Assessor (QSA) firm to work with and advise the MoJ, it's agencies and arm's length bodies (ALBs) on achieving and maintaining Payment Card Industry Data Security Standards (PCI DSS) compliance.

1.2 Ministry of Justice

The MoJ is one of the largest government departments, with around 95,000 people (including probation services) and a budget of £7.7 billion.

The MoJ works in partnership with the other government departments and agencies to reform the criminal justice system, to serve the public and support victims of crime. This includes HM Prisons and Probation Service (HMPPS) HM Courts & Tribunals Service (HMCTS), Legal Aid Agency (LAA), the Office of the Public Guardian (OPG).

- HMPPS is responsible for ensuring that people serve the sentences and orders handed out by courts, both in prisons and in the community. This includes responsibility for the running of prison services, probation services and rehabilitation services;

- HMCTS is responsible for the administration of criminal, civil and family courts and tribunals in England and Wales;

- LAA provides civil and criminal legal aid and advice in England and Wales for over 2 million people each year;

- OPG is an executive agency sponsored by the Ministry which protects people in England and Wales who many not have the mental capacity to make certain decisions themselves such as about their health and finance.

A list of all MoJ entities is listed at Schedule 1.

2 Background

MoJ entities currently accept and process card payments via various payment methods which includes but is not limited to telephone, face to face and internet payments. The infrastructure supporting card transactions and related reconciliations is complex and maintained by multiple Suppliers.

The MoJ currently receives Merchant Acquiring Services from Barclaycard and Worldpay and other Suppliers that facilitate and process payments on behalf of the relevant MoJ entity. These services are predominantly used by:

(1) HMCTS for the collection of courts and tribunal's fees, court fines and fixed penalties

(2) LAA for legal aid contributions, and

(3) HMPPS who utilise these services in a number of establishments (for example shops, museums or garages) attached to prisons.

2.1 Merchant Acquiring Services

An overview of the payment streams, transaction volumes and details of the current Merchant Acquirer Services Supplier can be found at Table 1.

Table 1 Overview of Payments

MoJ Entity	Merchant Acquirer	No. of outlets	Value of transactions per annum
HMCTS	Barclaycard	429	£331m
HMPPS	Barclaycard	4	£50k
HMPPS	Worldpay	77	£15m
LAA	Barclaycard	2	£3m
OPG	Worldpay	3	£17m

Table 2 Number of outlets by channels and entity:

	HMCTS	HMPPS	LAA	OPG
eCommerce solutions	173	1	n/a	1
MOTO via supplier such as Eckoh	11	n/a	1	1
MOTO via Merchant Acquirer web payment solutions	417	n/a	1	1
Face to Face	414	80	n/a	n/a

The department's strategy is to use Gov.UKPay for eCommerce solutions; however, there remain some older solutions which are utilising Merchant Acquirer's payment engines to facilitate the processing of payments.

3 Specifications

3.1 Supplier specifications

The Supplier shall be an independent data security firm that has been qualified by the PCI Security Standards Council (the Council) to validate an entity's adherence to PCI DSS.

The Supplier's QSA employees must have satisfied and continue to satisfy all QSA requirements to perform PCI DSS assessments, including certification and re-certification as required by the Council.

The Supplier and it's QSA employees shall be on the Council's list of approved companies as published on the Council's website https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors

The Supplier will assign a QSA to the MOJ to achieve continuity through the assessment process to achieve compliance with PCIDSS.

The Supplier should have experience in assessing the security of similar organisations.

3.2 Scope of Contract

The Supplier shall work with and provide advice to all relevant MoJ entities which take card payments (or are planning to) on how to achieve and maintain PCI DSS compliance. In doing this the Supplier will work with operational teams and the MoJ's DigiTech team to ascertain scope and establish where reasonable mitigating actions are already in place particularly in respect of data security across the department's IT networks. A list of all relevant MoJ entities is listed at Schedule 1.

The Supplier will work with the current or future merchant acquirers and other Suppliers who currently facilitate and process transactions for each MoJ entity. A list of the current merchant acquirers, which may be subject to change, can be found at Table 1 above.

The Supplier will provide advice on the MoJ's strategic approach to achieving compliance and minimising the burden of evidencing compliance.

3.3 Services

3.3.1 The QSA will:

- perform a PCI DSS security assessment of the MoJ cardholder data environment, report on findings and provide recommendations on remedial action to be taken to work towards achieving PCI DSS compliance based on the current PCI standards requirements as published on the PCI DSS council's website at https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security
- review and assess quarterly network scans (to be provided by DigiTech suppliers) and analysis of outputs
- advise on annual reporting requirements, complete and submit the relevant annual report along with any other supporting documents
- provide ongoing support, training and advice to MoJ entities on an ad hoc basis over the duration of the contract
- verify all technical information given by the merchant or service provider
- use independent judgement to confirm the standard has been met
- provide support and guidance during the compliance process
- be onsite for the duration of the assessment as required
- adhere to the PCIDSS Security Assessment Procedures
- validate the scope of the assessment
- evaluate compensating controls
- produce the final report

3.3.2 The Services shall include the following:

- **Pre-Assessment**

Scoping - review the areas, processes and technologies (where card holder data is stored, processed or transmitted) that have been identified by the MoJ entities as being in scope and verify scope i.e. determine if compensating controls removes it from scope or responsibility sits with the MoJ or a third-party contractor.

Gap Analysis - analyse and review policies and procedures to identify existing gaps and risks that may lead to non-compliance with PCI DSS.

Compensating Controls Analysis - conduct compensating controls analysis and document mitigations which are sufficient to address a gap.

Compliance Readiness Report - develop a strategic prioritised action plan and provide a compliance readiness report which documents the steps needed to (1) reduce the PCI DSS scope and (2) remediate gaps in compliance. Provide an executive summary presentation to key stakeholders.

- **Assessment**

Assessment - examine the compliance of system components and networks that are in scope following the testing procedures for each PCI DSS requirement listed as published at https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security.

Advising - provide advice on the use of the prioritised approach and achievement of milestones 1 to 6 (as per the PCI DSS Council checklist).

Reporting - report on progress with compliance to the Merchant Acquirer. Complete and submit the final PCI DSS Report on Compliance and any other supporting documentation e.g. toolsets used to document CDE, approach taken in determining scope, quarterly scan results and findings and observations as well as validation of all compensating controls.

- **Post-Assessment**

Advice and Training - provide ad-hoc advice on the impact of changes to PCI DSS requirements and actions required to remain compliant.

Quarterly Network Scans - review and analyse data and evidence from quarterly network scans, penetration testing and other security reports.

3.4 Management and Contract Administration

The Supplier shall appoint a contract manager who will be responsible for service delivery and act as a point of contact for the MoJ operational contract manager.

Th MoJ Commercial Contract Management team (CCMD) will support the operational contract manager with any commercial queries.

3.4 Location of Services

The Supplier shall be based at their office and it is expected that the QSA will work remotely for most of the period of engagement.

If the Supplier is required to attend meetings outside of Greater London then:

- any reasonable additional expenses (travel and subsistence) will need to be authorised by the MoJ Operational Contract Manager by signing of a timesheet or scope of works

- subsistence rates are expected to be based on the HMRC benchmark scale rates.

It is anticipated that the Supplier will be required to attend meetings at MoJ HQ in London (102 Petty France, Westminster or 10 South Colonnade, Canary Wharf). The MoJ shall not cover additional expenses in respect of travel, accommodation and subsistence to or within Greater London.

4 Contract Term

The contract term shall be 2 years. The initial engagement period will be 20 days over the contract term with an option to extend up to a further 10 days.

Schedule 1

Ministry of Justice

Executive Agencies:

- Criminal Injuries Compensation Authority
- HM Courts & Tribunals Service
- Her Majesty's Prison and Probation Service
- Legal Aid Agency
- Office of the Public Guardian

Executive non-department public body:

- Cafcass
- Criminal Cases Review Commission
- Judicial Appointments Commission
- Lega Services Board
- Parole Board
- Youth Justice Board for England and Wales

Advisory non-departmental public bodies and other public bodies:

For details visit https://www.gov.uk/government/organisations